EXHIBIT A

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

23 MAG 6718

In the Matter of a Warrant for Certain Content and Other Information Associated with the Google Accounts **charlie@withfrank.org, olivier@withfrank.org,** Maintained at Premises Controlled by Google LLC, USAO Reference No. 2022R01035

TO BE FILED UNDER SEAL

AGENT AFFIDAVIT

Agent Affidavit in Support of Application for a Search Warrant for Stored Electronic Communications

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

JEREMY ROSENMAN, being duly sworn, deposes and states:

I. Introduction

A. Affiant

1. I am a Special Agent in the United States Attorney's Office for the Southern District of New York (the "USAO" or "Investigating Agency"). I have been employed by the USAO since 2016. During my time with the USAO, I have participated in investigations of securities, wire, and bank fraud schemes, and have, among other things, conducted or participated in debriefings of witnesses, reviews of financial records, and the execution of search warrants. In particular, I have participated in the execution of search warrants involving physical premises, electronic devices, email accounts, and other electronic evidence.

B. Google, the TARGET GOOGLE ACCOUNTS, and the Subject Offenses

2. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. § 2703 for content and other information associated with:

The Google accounts **charlie@withfrank.org ("TARGET GOOGLE ACCOUNT-1")** and **olivier@withfrank.org ("TARGET GOOGLE ACCOUNT-2"),** (collectively, the "**TARGET GOOGLE ACCOUNTS**") are maintained and controlled by Google, LLC ("Google"), located at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in the attachments to the proposed warrants.

3. As detailed below, there is probable cause to believe that the **TARGET ACCOUNTS** contain evidence, fruits, and instrumentalities of a scheme to submit false statements and information about a company, TAPD, Inc., d/b/a Frank ("Frank"), in order to induce J.P. Morgan Chase ("JPMC") to acquire Frank for approximately $175 million and to cover up that scheme by continued false statements to JPMC, in violation of 18 U.S.C. §§ 1349 (conspiracy to commit bank and wire fraud); 1343 (wire fraud); 1344 (bank fraud); and 2 (aiding and abetting); and 15 U.S.C. §§ 78j(b) & 78ff, and 17 C.F.R. § 240.10b-5 (securities fraud) (collectively, the "Subject Offenses"). This affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers, as well as my training and experience concerning the use of email in criminal activity. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts I have learned during my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

C. Services and Records of Google

4. Based on my training and experience, I have learned the following about Google:

a. Google offers email services to the public. In particular, Google allows subscribers to maintain email accounts under domain names, such as gmail.com. A subscriber using Google's services can access his or her email account from any computer connected to the Internet.

b. Google maintains the following records and information with respect to every subscriber account:

i. *Email contents*. In general, any email (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on Google's servers unless and until the subscriber deletes the email. If the subscriber does not delete the email, it can remain on Google's computers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

ii. *Address book.* Google also allows subscribers to maintain the equivalent of an address book, comprising email addresses and other contact information of other email users.

iii. *Subscriber and billing information.* Google collects and maintains (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate email addresses. Google also maintains records concerning the date on which the account was created, the Internet protocol ("IP") [1] address of the user at the time of account creation, the current status of the account (*e.g.*, active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, Google maintains records of the subscriber's means and source of payment, including any credit card or bank account number.

[1] Based on my training and experience, I know that each electronic device connected to the Internet must be assigned a unique IP address so that communications from or directed to that electronic device are routed properly.

iv. *Device Information.* Google collects and maintains information identifying devices (including both computers and mobile devices) used to access accounts, including, for example, device serial number, a GUID or Global Unique Identifier, a phone number, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI").

v. *Cookie Data.* Google uses features to track the activity of users of their accounts, including whether or not the user of an account accesses other accounts at the provider using the same computer, or accesses accounts maintained by other companies while logged into an account. One of the ways Google does that is by using cookies, a string of characters stored on the user's computer or web browser that is recognized by Google when a computer visits its site or logs into an account.

vi. *Transactional information.* Google also typically retains certain transactional information about the use of each account on its system. This information can include records of login (*i.e.*, session) times and durations and the methods used to connect to the account (such as logging into the account through Google's website).

vii. *Customer correspondence.* Google also typically maintains records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account.

viii. *Preserved and backup records*. Google also maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving

a preservation request from the Government pursuant to 18 U.S.C. § 2703(f). Google may also maintain backup copies of the foregoing categories of records pursuant to its own data retention policy.

c. In addition, Google also maintains records with respect to other Google Services, which it stores in connection with subscriber accounts, which typically include the following:

i. *Google Analytics*. Google Analytics is a platform that collects data from a Google account holder's website and/or apps to create reports with metrics regarding the use of the website. To measure a website, the Google account holder first has to create a Google Analytics account. Then the Google account holder adds a small piece of JavaScript measurement code to each page on his or her website. Every time a person visits a webpage, the tracking code will collect pseudonymous information about how that visitor[2] interacted with the page. For the Google Store, the measurement code could show how many visitors visited a page that sells drinkware versus a page that sells houseware. Or it could tell Google how many visitors bought an item like an Android doll by tracking whether they made it to the purchase-confirmation page. The measurement code will also collect information from the browser like the language setting, the type of browser (such as Chrome or Safari), and the device and operating system on which the browser is running. It can even collect the "traffic source," which is what brought visitors to the site in the first place. This might be a search engine, an advertisement they clicked on, or an email marketing campaign. When the measurement code collects data, it packages that information and sends it to Google Analytics to be processed into reports. When Analytics processes data, it aggregates and organizes the data based on particular criteria like whether a visitor's device is mobile or desktop, or which browser they're using. Google Analytics also provides configuration

[2] Google Analytics collects a number of metrics which are specifically defined by Google.

settings that allow the Google account holder to customize how that data is processed. For example, the Google account holder could want to apply a filter so that the data does not include any internal company traffic or developer traffic. Once Analytics processes the data, it is stored in a database where it cannot be changed. Once the data has been processed and stored in the database, it appears in Google Analytics as reports.

ii. *Google Drive content*. Google provides users with a certain amount of free "cloud" storage, currently 15 gigabytes, through a service called "Google Drive" (users can purchase a storage plan through Google to store additional content). Google account holders can purchase enhanced storage capacity for an additional monthly fee. Google account holders can use their Google Drive to store email, attachments, videos, photographs, documents, and other content "in the cloud," that is online. An account holder can access content stored on Google Drive by logging into his or her Google account through any computer or other electronic device that is connected to the Internet. Account holders can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files. Google Drive is integrated with, and can include, files created or edited in collaborative content creation apps like Google Docs, Sheets, and Slides (described below).

ii. *Google Docs, Google Sheets, Google Slides*. Google provides account holders with the ability to write, edit, and collaborate on various documents with other Google users through a service called "Google Docs." Account holders can use Google Docs to create online documents that can be stored on or saved to the user's Google Drive. Google Sheets and Google Slides operate the same way, but for spreadsheets and online slideshows, respectively.

iii. *Google Photos*. Google provides account holders with a certain amount of free storage for photographs, through a service called Google Photos, which allows account

holders to manually store photographs and videos, and which automatically uploads photographs and videos taken by registered mobile devices. Google also retains the metadata—or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means of its creation, the purpose of the data, among other data—for photos and videos that are uploaded to Google, including to Google Photos. This metadata includes what is known as exchangeable image file format (or "Exif") data, and can include GPS location information for where a photo or video was taken.

iv. *Google Calendar*. Google provides account holders with an online calendar, in which they can add appointments, events, and reminders, which are synchronized across registered computers and mobile devices. Account holders can share their calendars with other users, allowing the maintenance of joint calendars.

v. *Google Chats and Google Hangouts content*. Google allows subscribers to engage in "chat" sessions in an instant messaging format with other Google users, the transcripts of which are generally stored in an account holder's email content. Similarly, Google allows users to engage in enhanced chat sessions, called Hangouts, which permit the sharing of additional content such as videos, sounds, and images. In general, Hangouts content is stored separately from an account holder's email and chat content.

vi. *Location History data*. Google maintains recent location data, collected periodically, from mobile devices that are logged into or have used applications (or "apps") or services provided by Google. For example, Google collects information collected from Global Positioning System ("GPS"), Wi-Fi networks, cell site locations, and mobile networks to estimate a user's location. Google apps and services also allow for location reporting, which allows Google

to periodically store and use a device's most recent location data in connection with a Google account.

vii. *Google Payments*. Google allows for the storage of payment information associated with a Google Account, including credit cards and bank accounts, and contains information about all transactions made with a Google account, allowing for the payment for goods (such as those purchased through Google Shopping) and bills, among other features.

viii. *Chrome Browser and Search History*. Google stores information regarding user Internet browser activity when a Google account holder is logged into his or her account, which includes logging information about websites viewed by the account holder, Internet search queries in the Google Internet search engine available at http://www.google.com, and also maintains lists of bookmarks maintained by the user so that he or she can quickly access frequently viewed websites.

D. Jurisdiction and Authority to Issue Warrant

5. Pursuant to 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as Google, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

6. A search warrant under § 2703 may be issued by "any district court of the United States (including a magistrate judge of such a court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

7. When the Government obtains records under § 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding

the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

II. Probable Cause

A. Probable Cause Regarding the Commission of the Subject Offenses

Overview of the Fraud Scheme

8. On or about March 31, 2023, the Honorable Robert W. Lehrburger authorized a criminal complaint (the "Complaint") charging CHARLIE JAVICE, the former CEO of Frank, with 18 U.S.C. §§ 1349 (conspiracy to commit bank and wire fraud); 1343 (wire fraud); 1344 (bank fraud); and 2 (aiding and abetting); and 15 U.S.C. §§ 78j(b) & 78ff, and 17 C.F.R. § 240.10b-5 (securities fraud), and issued a warrant for JAVICE's arrest. The Complaint is attached hereto as Exhibit 1 and incorporated as if set forth fully herein.

9. On or about May 18, 2023, a grand jury in this District issued an Indictment charging JAVICE with the same charges as contained in the Complaint. On or about July 12, 2023, a grand jury in this District issued a superseding indictment ("Superseding Indictment") adding AMAR as a defendant to all four counts. The Superseding Indictment is attached hereto as Exhibit 2 and incorporated as if set forth fully herein.

10. As set forth in the Complaint, and as I have learned from my review of records from JPMC, other third parties involved in the acquisition of Frank by JPMC, and interviews of witnesses:

a. JAVICE founded the company Frank in or about 2017 as a for-profit company that would assist college students with federal financial aid. JAVICE was the CEO of Frank, and OLIVIER AMAR—who is identified as "CC-1" in the Complaint—was the Chief Growth Officer of Frank. *See* Ex. 1 ¶¶ 9, 13, 15-16.

b. In or about 2021, JAVICE and AMAR began to pursue the sale of Frank to a larger financial institution. Two major banks (JPMC and Capital One) expressed interest and began acquisition processes with Frank. JAVICE represented repeatedly to those banks that Frank had 4.25 million customers or "users." JAVICE explicitly defined "users"—to both banks—as individuals who had signed up for an account with Frank and for whom Frank therefore had at least four identified categories of data (*i.e.*, first name, last name, email address, and phone number). In fact, Frank had less than 300,000 users. *See* Ex. 1 ¶¶ 10, 18-19, 22-23.

c. When JPMC sought to verify the number of Frank's users and the amount of data collected about those users—information that was critical to JPMC's decision to move forward with the acquisition process—JAVICE fabricated a data set, which was provided to a third-party validator that verified certain information for JPMC. *See* Ex. 1 ¶¶ 11, 21, 24-26.

d. In reliance on JAVICE's fraudulent representations about Frank's users, JPMC agreed to purchase Frank for $175 million. JAVICE and AMAR made millions of dollars from the acquisition. *See* Ex. 1 ¶¶ 12, 31.

e. Unbeknownst to JPMC, at or about the same time that JAVICE was creating the fabricated data set, JAVICE and AMAR sought to purchase, on the open market, *real* data for over 4.25 million college students in an effort to cover up their lies. JAVICE and AMAR succeeded in purchasing a data set of 4.5 million students for $105,000, but it did not contain all the data fields that JAVICE had represented to JPMC were maintained by Frank. JAVICE then purchased an additional set of data on the open market, in order to augment the data set of 4.5 million users. After

JPMC acquired Frank, JPMC employees asked JAVICE and AMAR to provide the data set of Frank users so that JPMC could begin a marketing campaign to those users. In response, JAVICE provided what was supposedly Frank's user data. In fact, JAVICE provided the data she and AMAR had purchased on the open market, at a small fraction of the price that JPMC paid to acquire Frank and its purported users. *See* Ex. 1 ¶¶ 13, 28-30.

11. The events set forth above resulted in numerous court proceedings, including (as relevant here) a civil lawsuit filed by JPMC in January 2023 against Javice and Amar. *See J.P. Morgan Chase Bank, N.A. v. Charlie Javice and Olivier Amar*, No. 22 Civ. 01621 (JDW) (D. Del.). On or about February 27, 2023, Javice filed an answer and counterclaim. In her publicly filed counterclaim, Javice claimed that when she and others stated that Frank had 4.25 million "users," they were not referring to individuals who had signed up for an account with Frank and for whom Frank therefore had at least four identified categories of data, but, rather, to "cumulative website users who viewed website content pertaining to FAFSA [*i.e.*, visitors to the website]." (*See* Javice Answer and Counterclaim ¶¶ 47, 50).

12. Based on my review of documents provided by JPMC pursuant to legal process, I have learned that specific representations were made to JPMC not only about the number of "users" but also about the web traffic numbers for Frank's website. For example, in or about July 2023, due diligence sessions for the potential Frank acquisition took place at JPMC's headquarters in New York City. At those sessions, JAVICE fielded questions from JPMC executives about Frank. Notes of that meeting indicate that JPMC was told that the number of "users" (a person for whom

Frank had collected first name, last name, email address, and phone number) was 4.25 million and that the number of Frank website visitors was 35 million.

The TARGET GOOGLE ACCOUNTS

13. Based on documents provided by Google[3] pursuant to legal process, I have learned the following, set forth in substance and in part:

a. **TARGET GOOGLE ACCOUNT-1** (charlie@withfrank.org) was created on or about July 13, 2016 and subscribed to in the name "Charlie Javice."

b. **TARGET GOOGLE ACCOUNT-1** used a number of Google services including Google Analytics, Google Docs, and Google Drive.

c. The "end of service" date for **TARGET GOOGLE ACCOUNT-1** is September 13, 2022.

d. **TARGET GOOGLE ACCOUNT-2** (olivier@withfrank.org) was created on or about February 28, 2017 and subscribed to in the name "Olivier Amar."

e. **TARGET GOOGLE ACCOUNT-2** used a number of Google services including Google Analytics, Google Docs, and Google Drive.

f. The "end of service" date for **TARGET GOOGLE ACCOUNT-2** is September 13, 2022.

g. Google identified the Google Analytics platform for the Frank website as a "property" of both **TARGET GOOGLE ACCOUNT-1** (charlie@withfrank.org) and **TARGET GOOGLE ACCOUNT-2** (olivier@withfrank.org), along with a number of other Frank-

[3] Although the TARGET GOOGLE ACCOUNTS have the domain "withfrank.org," they are both hosted by Google.

associated "properties," including "frankTesting," "Frank-staging," and "Acadeum – Shopify-Test."[4]

The Use of the TARGET GOOGLE ACCOUNTS in the Scheme

14. Based on my training and experience, and my review of information from Google about Google Analytics,[5] I have learned the following, set forth in substance and in part:

a. Google Analytics collects metrics for "Users" and "Sessions" (among other metrics).

b. The "sessions" metrics tracks the number of sessions that began on a particular website or application. A "session" is defined as "a period of time during which a user interacts with [the Google account holder's] website or app. . . . By default, a session ends (times out) after 30 minutes of user inactivity. There is no limit to how long a session can last."

c. A "user" in the context of Google Analytics is defined as "[t]he number of distinct users who visited [the Google account holder's] website or application."

15. Based on my interview with a former Frank employee who worked on Frank's "Growth" team ("Employee-1"), I have learned the following, set forth in substance and in part:

[4] Acadeum was a vendor for a part of Frank's business which sold online college courses.

[5] As discussed above at paragraph 4(c)(i), Google Analytics is a platform that collects data from a Google user's website and/or apps to create reports with metrics regarding the use of the website. To measure a website, the Google user first has to create a Google Analytics account. Then the Google user adds a small piece of JavaScript measurement code to each page on his or her website. Every time a user visits a webpage, the tracking code will collect pseudonymous information about how that user interacted with the page. The measurement code will also collect information from the browser like the language setting, the type of browser (such as Chrome or Safari), and the device and operating system on which the browser is running. When the measurement code collects data, it packages that information up and sends it to Google Analytics to be processed into reports. When Analytics processes data, it aggregates and organizes the data based on particular criteria like whether a user's device is mobile or desktop, or which browser they're using. Once Analytics processes the data, it is stored in a database where it cannot be changed. Once the data has been processed and stored in the database, it appears in Google Analytics as reports.

a. Frank tracked a number of metrics related to company growth. Among other metrics, Frank's Growth team, led by AMAR, tracked both website traffic (the number of people who landed on the Frank website or who interacted with the website in certain ways) and the number of people who created accounts with Frank.

b. Frank tracked website traffic primarily through Google Analytics. The number of people who created accounts on the Frank website was also tracked in Google Analytics (among other platforms).

16. Based on my training and experience, and my participation in this investigation, I know that the metrics for website traffic (*i.e.*, people who visited a website) would be greater than the number of people who signed up for an account on the same website (the latter being a subset of the former).

17. Based on my review of emails produced by JPMC pursuant to legal process,[6] I have learned the following, set forth in substance and in part:

a. Both **TARGET GOOGLE ACCOUNTS** were associated with, and had access to, Frank's Google Analytics platform. Both **TARGET GOOGLE ACCOUNTS** also received automated updates from Google Analytics regarding website traffic metrics for the Frank website.

b. For example, on or about June 8, 2021, Google Analytics sent an automated email to **TARGET GOOGLE ACCOUNT-1** (charlie@withfrank.org) with the Subject heading: "In May, you had 118.5K users visit your website (Google Analytics)" and, in the body, a link to the "Full Report" from Google Analytics for https://withfrank.org.

[6] JPMC acquired Frank's computer servers when it acquired the company. As a result, JPMC possesses email content from the **TARGET GOOGLE ACCOUNTS**. However, the **TARGET GOOGLE ACCOUNTS** used other Google Services (e.g., Google Drive and Google Analytics) to which JPMC does not have access.

c. As another example, on or about August 3, 2021, Google Analytics sent an automated email to **TARGET GOOGLE ACCOUNT-2** (olivier@withfrank.org) with the Subject heading: "In July, you had 123.9K users visit your website (Google Analytics)" and, in the body, a link to the "Full Report" from Google Analytics for "https://withfrank.org."

d. AMAR and JAVICE also communicated with each other about Google Analytics data through documents shared on Google Drive. For example, on or about June 18, 2021—while Frank was in an acquisition process with Capital One and shortly before the start of the acquisition process with JPMC—JAVICE commented on a document shared in Google Drive, "@olivier@withfrank.org - can you grab google analytics sessions graph. and copy paste here."

18. Based on my review of emails produced by JPMC pursuant to legal process, I have learned the following about the use of Google Drive by the **TARGET GOOGLE ACCOUNTS**, set forth in substance and in part:

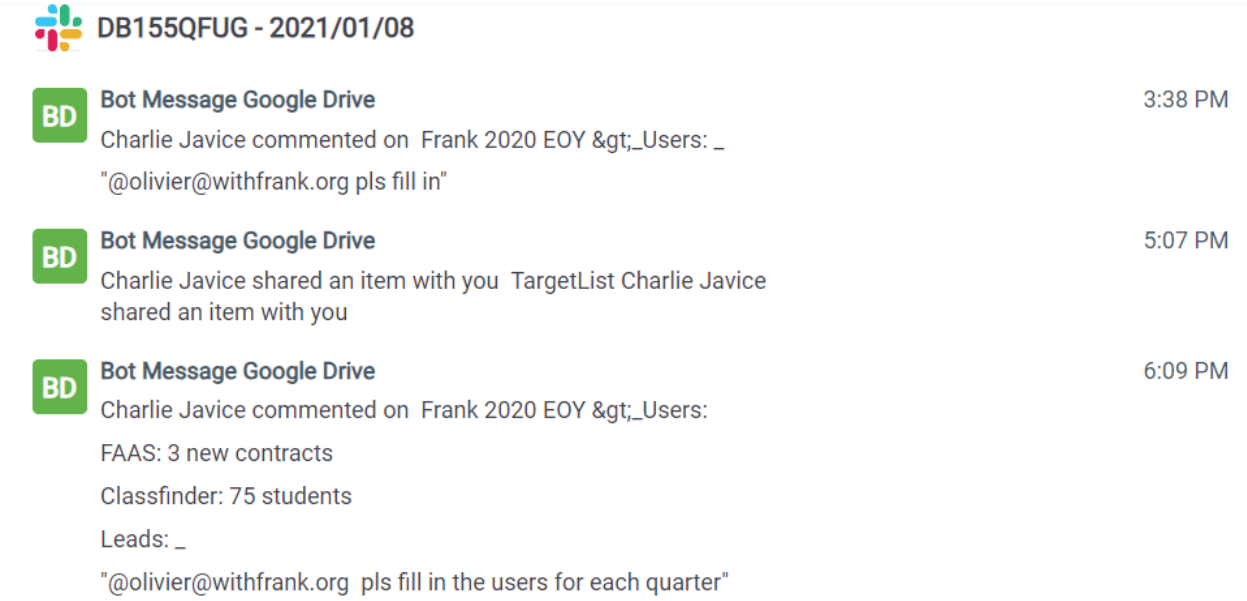
a. Both **TARGET GOOGLE ACCOUNTS** used Google Drive to share, collaborate on, and comment on, documents related to Frank, including documents related to the number of Frank "users."[7]

b. For example, on or about January 5, 2021—shortly before JAVICE formally engaged an investment advisory firm to represent Frank in seeking an acquirer—**TARGET GOOGLE ACCOUNT-1** (charlie@withfrank.org) sent an automated email to another Frank employee ("Frank Employee-1") via Google Slides with subject "2020_EOY." The body of the email stated, "Charlie Javice added comments to the following document . . . 2020_EOY." The body of the email also indicated that JAVICE had commented on, and been questioned about, the

[7] This is consistent with information obtained from Google pursuant to legal process identifying Google Drive as a Google service used by both of the **TARGET GOOGLE ACCOUNTS**.

meaning of "user" in the due diligence process. Frank Employee-1 asked, in reference to the document, "Are these users or site visitors?" To which JAVICE responded, "we are calling users visitors in our new hierarchy. then its accounts." Frank Employee-1 also asked, in reference to the word "served" in the document, "How are we defining this word . . . in diligence?" JAVICE responded, "users defined as people who used our website."

c. A few days later, on or about January 8, 2021, a Slack channel[8] with automated messages from Google Drive indicated that JAVICE had commented the following on a document in Google Drive entitled "Frank 2020 EOY >_Users:_": "@olivier@frankfafsa.com pls pull the user data." JAVICE also asked AMAR, for that same document, to "pls fill in" and "pls fill in the users for each quarter," as depicted below:



d. As another example, on or about June 24, 2021, **TARGET GOOGLE ACCOUNT-2** (olivier@withfrank.org) received an email from **TARGET GOOGLE**

[8] Slack is a messaging platform frequently used by companies and organizations for workplace communication. Slack organizes conversations into dedicated spaces called "channels." Different channels can have different participants and subject matters.

ACCOUNT-1 (charlie@withfrank.org) "via Google Sheets" stating that JAVICE "has invited you to edit the following spreadsheet:" "User_Breakdown_CJ_v2." The "CJ" in the document title appears to represent JAVICE's initials.

e. Based on my review of emails provided by Frank's investment advisory firm ("Investment Advisory Firm-1") pursuant to legal process, I know that JAVICE sent an Excel spreadsheet with an identical title as the Google Sheets spreadsheet described in the paragraph above ("User_Breakdown_CJ_v2") to Investment Advisory Firm-1 to add to the "data room."[9] Notably, this document contained the misrepresentation that Frank had "4,265,085" individuals who had at least started a FAFSA. As described in paragraph 22(j) of the Complaint, the true number was less than 150,000.

f. As another example of the use of Google Drive by the **TARGET GOOGLE ACCOUNTS** in the scheme, on or about August 1, 2021, **TARGET GOOGLE ACCOUNT-1** sent an automated email via Google Docs to **TARGET GOOGLE ACCOUNT-2**, with a carbon copy to the Frank employee identified as "Engineer-1" in the Complaint. The body of the email stated that JAVICE had invited AMAR to edit a document entitled "Data_Request" with the notation "user session data." The sharing of this document is notable because, as described in the Complaint, August 1, 2021 was the date on which JPMC sent JAVICE its request to validate Frank's user data (*see* Complaint ¶ 21) and the date on which JAVICE first asked Engineer-1 to create a synthetic data set (*see* Complaint ¶ 22(c)). The date, participants, and contents of the

[9] In the context of an acquisition, a "data room" is a collection of documents about a company seeking to be acquired. The documents can range in subject matter from human resources documents to information about the company's core business. The documents are reviewed by potential buyers and/or investors as part of the due diligence process.

email indicate that the document shared by JAVICE with AMAR related to the request to Engineer-1 to generate a synthetic data set.

B. Probable Cause for the TARGET ACCOUNTS

19. Accordingly, I submit that there is probable cause to believe that the **TARGET GOOGLE ACCOUNTS** will contain evidence and/or instrumentalities of the Subject Offenses. Specifically, as described in paragraphs 14-17, there is probable cause to believe that the **TARGET GOOGLE ACCOUNTS** will contain evidence of the website traffic numbers for the Frank website, the number of registered Frank accounts, and JAVICE and AMAR's knowledge of those metrics. That content will tend to show, among other things, whether the representations made to JPMC about the number of website visitors were accurate and would also shed light on JAVICE and AMAR's representations regarding the number of registered accounts.

20. In addition, as described in paragraph 18, there is probable cause to believe that the **TARGET GOOGLE ACCOUNTS** will contain evidence of documents related to the due diligence process for the potential Frank acquisition (including documents which were later provided to potential buyers), documents related to the number of Frank "users" (registered accounts or otherwise), and comments and/or edits to those documents reflecting JAVICE and/or AMAR's knowledge of, or involvement in, a scheme to misrepresent facts to potential buyers in the course of Frank's acquisition.

21. Based on my training and experience, I have learned that search history, which Google maintains, can also provide important evidence of identity, state of mind, or criminal activity. In my training and experience, individuals involved in fraud schemes often search for terms relating to the fraud or to covering up the fraud (for example, "how to wipe a hard drive," criminal statutes, or names of victims). Individuals engaged in fraud often search for terms relevant to the particular fraud itself. For example, as described in paragraph 22(e) of the Complaint, before the call with

Engineer-1, JAVICE sent Engineer-1 an email with a link to a website that explained how "to generate synthetic data that is similar to the actual data in terms of statistics and demographics." Based on my training and experience, I submit that JAVICE may have searched for websites relating to synthetic data in order to find that website—and that those search terms would provide evidence about JAVICE's knowledge, intent, and state of mind.

22. Because certain of the key misrepresentations to JPMC involved "cumulative" numbers of users or website visitors, and because, as alleged in paragraph 32 of the Complaint, the fraud on JPMC continued after the acquisition of Frank, I respectfully submit that there is probable cause to believe that the contents of the **TARGET GOOGLE ACCOUNTS** (including documents, spreadsheets, and analytics data) from their inception[10] to September 13, 2022 (the "end of service" date for both accounts) constitute evidence and/or instrumentalities of the Subject Offenses, including evidence of misrepresentations to JPMC both before and after the acquisition and evidence of JAVICE, AMAR and/or others' knowledge of and involvement in those misrepresentations. In addition, documents and records showing consistencies or inconsistencies in how JAVICE, AMAR or other Frank employees defined or understood the term "user" *prior* to the acquisition process would be relevant to JAVICE and AMAR's intent and state of mind in how they represented that term during or after the acquisition process.

23. In my training and experience, the Providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers,

[10] Based on my participation in this investigation (including my review of multiple emails to and from the **TARGET GOOGLE ACCOUNTS**) and as is clear from the domain of the **TARGET GOOGLE ACCOUNTS** (withfrank.org), I know that the **TARGET GOOGLE ACCOUNTS** were created for use relating to Frank's business.

alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

24. In my training and experience, the Provider typically retains certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, the Provider often has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a particular Google account.

25. In my training and experience, in some cases, Google account users will communicate directly with Google about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. The Provider typically retains records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users and the purposes for which the account was used.

26. Individuals who participate in criminal schemes, such as bank fraud schemes, commonly use electronic communications to communicate with co-conspirators and victims in furtherance of the scheme. Based on my training and experience, and my participation in this investigation, I know that JAVICE and AMAR did use electronic communications to communicate about the fraud scheme, and used different platforms for electronic communications (e.g., email and Slack). One example of such a communication is described above at paragraph 18(f).

27. Based on my training and experience, I know that when an individual participates in a criminal scheme, photographs or videos stored in that individual's electronic accounts, such as email accounts or photo/video libraries, often contain evidence of that scheme because such photographs or videos can provide evidence of relationships between participants in the scheme. For example, photographs or videos may evidence joint vacations, social interactions, and potentially provide insight into the frequency of contacts between individuals.

28. Furthermore, historical location data collected by a user's electronic accounts can be relevant to establishing that user's participation in a criminal conspiracy, such as by showing when the relevant actors were together in person and thus how and when information was transmitted.

29. Based on my training and experience, I know that individuals who engage in criminal schemes commonly maintain electronic records relating to their schemes, such as contact information for co-conspirators, records of fraudulent documents or emails, and financial account statements. These materials can be easily moved between an individual's electronic storage accounts, such as by email and file sharing and transfers between accounts (such as a Google Drive account).

30. Based on my training and experience, I also know that, where electronic messages or other electronic files are used in furtherance of criminal activity, evidence of the criminal activity

can often be found months or even years after it occurred. This is typically true because electronic files can be stored on computer servers for years at little or no cost and users thus may have little incentive to delete data that may be useful to consult in the future.

31. As explained herein, information stored in connection with an email or other online account from its inception may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described above, the Providers typically log the Internet Protocol (IP) addresses from which users access their accounts, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation (this can be relevant to, for example, placing an individual at a particular meeting). This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). As described above, search history, which Google maintains, can also provide important evidence of identity, state of mind, or criminal

activity. Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting documents in an effort to conceal them from law enforcement).

32. In my training and experience, evidence of who was using a particular Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. In addition, the stored communications and files connected to a Google account may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, transaction information, online searches, and documents, which are stored in different Google services (including Google Drive, Google Docs, Google Photos, Google Calendar, Google Chats, Google Hangouts, Google Photos, Web and Search History, and Google Payments) are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

33. Based upon the foregoing, I respectfully submit there is probable cause to believe that information stored on Google's servers associated with the **TARGET ACCOUNTS**, **(collectively, "the Subject Accounts")** will contain evidence, fruits, and instrumentalities of the Subject Offenses, as more fully described in Section II of Attachment A to the proposed warrants.

34. In particular, I seek authorization to search the Subject Accounts from their inception to September 13, 2022 for all records relating to a scheme to submit false statements and

information about a company, Frank, in order to induce JPMC to acquire Frank for approximately $175 million and to cover up that scheme by continued false statements to JPMC, in violation of 18 U.S.C. §§ 1349 (conspiracy to commit bank and wire fraud); 1343 (wire fraud); 1344 (bank fraud); and 2 (aiding and abetting); and 15 U.S.C. §§ 78j(b) & 78ff, and 17 C.F.R. § 240.10b-5 (securities fraud), consisting of the following:

a. Information identifying the user of the Subject Accounts and his or her location, and the individuals involved in the Subject Offenses, including photographs or videos depicting the user of the Subject Accounts and/or the relationships between individuals involved in the Subject Offenses, communications with individuals that the user of the Subject Accounts trusts, and information that can be used to ascertain the identity of the user of the Subject Accounts, such as travel information, receipts for online purchases, and payment information, or other communications with social network websites or third party service providers;

b. Evidence of (i) documents and communications relating to the Subject Offenses, such as pitch decks to potential investors/buyers, documents added or prepared for Frank's "data room," spreadsheets reflecting the number of registered accounts or website visitors; (ii) drafts or different versions of the same, including comments to those drafts; and (iii) documents and communications making reference to or containing discussion of the commission of the Subject Offenses;

c. Google Analytics records related to Frank's website or user numbers, and any communications regarding Frank's website traffic, registered user accounts, or misrepresentations about Frank's website traffic or registered user accounts;

d. Documents or records relating to the use or definition of the term "user" at Frank;

e. Google Drive, Google Docs, Google Sheets, or Google Slides records relating to Frank's website traffic, account sign ups, or Frank's acquisition by JPMC or other potential acquiring companies and any related due diligence, preparation, or analysis;

f. Search and web history records related to the Subject Offenses including, if applicable, web and application activity history (including search terms), device information history, and location history; and

g. Evidence concerning any other online accounts or any computer devices where evidence falling within the foregoing categories could be stored, including any passwords or encryption keys needed to access such evidence.

III. Review of the Information Obtained Pursuant to the Warrant

35. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrant requested herein will be transmitted to the Provider, which shall be directed to produce a digital copy of any responsive records to law enforcement personnel within 14 days from the date of service. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will retain the records and review them for evidence, fruits, and instrumentalities of the Subject Offenses as specified in Section III of Attachment A to the proposed warrant. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

36. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all emails within the Subject Accounts. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

IV. Conclusion

37. While JAVICE and AMAR have been publicly charged, the full scope of the Government's investigation has not been publicly disclosed. Therefore, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrants and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

38. Based on the foregoing, I respectfully request that the Court issue the warrant sought herein pursuant to the applicable provisions of the Stored Communications Act, 18 U.S.C. § 703(b)(1)(A) (for contents) and § 2703(c)(1)(A) (for records and other information), and the relevant provisions of Federal Rule of Criminal Procedure 41.

/s/ Jeremy Rosenman, by SDA with permission

Special Agent Jeremy Rosenman
United States Attorney's Office
Southern District of New York

Sworn to me through the transmission of this
Affidavit by reliable electronic means, pursuant to
Federal Rules of Criminal Procedure 41(d)(3) and 4.1, this
6th day of October, 2023

HONORABLE STEWART D. AARON
United States Magistrate Judge
Southern District of New York

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

23 MAG 6718

In the Matter of a Warrant for Certain Content and Other Information Associated with the Google Accounts **charlie@withfrank.org, olivier@withfrank.org,** Maintained at Premises Controlled by Google LLC, USAO Reference No. 2022R01035

SEARCH WARRANT

TO: Google LLC ("Provider")

United States Attorney's Office for the Southern District of New York ("Investigative Agency")

1. Warrant. Upon an affidavit of Special Agent Jeremy Rosenman of Southern District of New York, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds there is probable cause to believe the Google accounts

charlie@withfrank.org and **olivier@withfrank.org**

maintained at premises controlled by the Provider, contain evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 21 days of the date of service of this Warrant and Order, the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A. The Government is required to serve a copy of this Warrant on the Provider within 14 days of the date of issuance.

The Warrant may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

Dated: New York, New York
October 6, 2023

2:25 p.m.
Time Issued

HONORABLE STEWART D. AARON
UNITED STATES MAGISTRATE JUDGE
Southern District of New York

Google Search Attachment A

I. Subject Account and Execution of Warrant

This warrant is directed to Google LLC (the "Provider") headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043, and applies to certain content and other information within the Provider's possession, custody, or control associated with the following email accounts:

charlie@withfrank.org and **olivier@withfrank.org**

(the "Subject Accounts").

A law enforcement officer will serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below.

II. Information to be Produced by the Provider

To the extent within the Provider's possession, custody, or control, the Provider is directed to produce the following information associated with the Subject Accounts from their inception through September 13, 2022:

a. *Google Analytics*. All Google Analytics files and contents associated with the Subject Accounts.

b. *Google Services information.* The files and contents with the account related to any Google Service, including Google Drive, Google Docs, Google Sheets, Google Slides, Google Photos, Google Chats, Google Photos, and Web and Search History.

c. *Location History data*. All location data collected from devices that are logged into or have used applications (or "apps") or services provided by Google.

d. *Subscriber and payment information*. All subscriber and payment information regarding the Subject Accounts, including but not limited to name, username, address, telephone number, alternate email addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

e. *Device Information.* Any information identifying the device or devices used to access each of the Subject Accounts, including a device serial number, a GUID or Global Unique Identifier, a phone number, serial numbers, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"), and any other information regarding the types of devices used to access the Subject Accounts.

f. *Information Regarding Linked Accounts, Including Accounts Linked by Cookie.* Any information identifying accounts that are associated or connected to the Subject Accounts, including specifically by Cookie, Google Account ID, Android ID, or other account or device identifier.

g. *Transactional records*. All transactional records associated with the Subject Accounts, including any IP logs or other records of session times and durations.

h. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Accounts, including complaints, inquiries, or other contacts with support services and records of actions taken.

i. *Preserved or backup records.* Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. § 2703(f) or otherwise.

III. Review of Information by the Government

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of a scheme to submit false statements and information about a company, Frank, in order to induce JPMC to acquire Frank for approximately $175 million and to cover up that scheme by continued false statements to JPMC, in violation of 18 U.S.C. §§ 1349 (conspiracy to commit bank and wire fraud); 1343 (wire fraud); 1344 (bank fraud); and 2 (aiding and abetting); and 15 U.S.C. §§ 78j(b) & 78ff, and 17 C.F.R. § 240.10b-5 (securities fraud), consisting of the following:

a. Information identifying the user of the Subject Accounts and his or her location, and the individuals involved in the Subject Offenses, including photographs or videos depicting the user of the Subject Accounts and/or the relationships between individuals involved in the Subject Offenses, communications with individuals that the user of the Subject Accounts trusts, and information that can be used to ascertain the identity of the user of the Subject Accounts, such as travel information, receipts for online purchases, and payment information, or other communications with social network websites or third party service providers;

b. Evidence of (i) documents and communications relating to the Subject Offenses, such as pitch decks to potential investors/buyers, documents added or prepared for Frank's "data room," spreadsheets reflecting the number of registered accounts or website visitors; (ii) drafts or different versions of the same, including comments to those drafts; and (iii) documents and communications making reference to or containing discussion of the commission of the Subject Offenses;

c. Google Analytics records related to Frank's website or user numbers, and any communications regarding Frank's website traffic, registered user accounts, or misrepresentations about Frank's website traffic or registered user accounts;

d. Documents or records relating to the use or definition of the term "user" at Frank;

e. Google Drive, Google Docs, Google Sheets, or Google Slides records relating to Frank's website traffic, account sign ups, or Frank's acquisition by JPMC or other potential acquiring companies and any related due diligence, preparation, or analysis;

f. Search and web history records related to the Subject Offenses including, if applicable, web and application activity history (including search terms), device information history, and location history; and

g. Evidence concerning any other online accounts or any computer devices where evidence falling within the foregoing categories could be stored, including any passwords or encryption keys needed to access such evidence.